



COPY OF PAPERS  
ORIGINALLY FILED

2661  
#  
3

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Sjoblom

Serial No.: 10/083,680

Group No.: 2661

Conf. No. 9437

Filed: February 25, 2002

Examiner:

For: Ordered Delivery of Intercepted Data

RECEIVED

APR 23 2002

Commissioner of Patents and Trademarks

Washington, D.C. 20231

Technology Center 2600

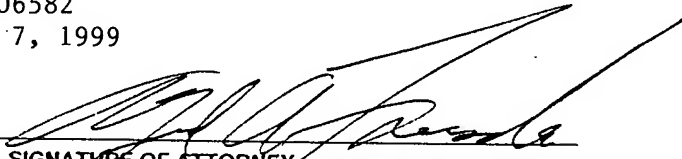
TRANSMITTAL OF CERTIFIED COPY

Attached please find the certified copy of the foreign application from which priority is claimed for this case:

Country : EP  
Application Number : PCT/EP99/06582  
Filing Date : September 7, 1999

Reg. No. 27,550

Tel. No. (203) 261-1234

  
SIGNATURE OF ATTORNEY

Alfred A. Fressola

Type or print name of attorney

WARE, FRESSOLA, VAN DER SLUYS & ADOLPHSON

P.O. Address

755 Main Street, PO Box 224

Monroe CT 06468

NOTE: The claim to priority need be in no special form and may be made by the attorney or agent if the foreign application is referred to in the oath or declaration as required by § 1.63.

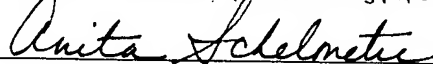
CERTIFICATE OF MAILING (37 CFR 1.8a).

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to the: Commissioner of Patents and Trademarks, Washington, D.C. 20231.

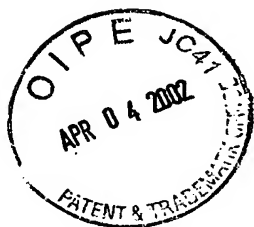
Date: March 27, 2002

Anita Schelmetic

(Type or print name of person mailing paper)



(Signature of person mailing paper)



**RECEIVED**

APR 23 2002

Technology Center 2600

**Bescheinigung**

**Certificate**

**Attestation**

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten internationalen Patentanmeldung überein.

The attached documents are exact copies of the international patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet international spécifiée à la page suivante.

Den Haag, den  
The Hague,  
La Haye, le

25.02.02

Der Präsident des Europäischen Patentamts  
Im Auftrag  
For the President of the European Patent Office  
Le Président de l'Office européen des brevets  
p. o.

  
Mme. C. Rossi

Patentanmeldung Nr.  
Patent application no.  
Demande de brevet n°

PCT/EP 99/06582



Anmeldung Nr.: PCT/EP 99/06582  
Application no.:  
Demande n°:

Anmelder: 1. NOKIA TELECOMMUNICATIONS OY - Espoo, Finland  
Applicant(s): 2. SJÖBLOM, Kai - Espoo, Finland  
Demandeur(s):

Bezeichnung der Erfindung:  
Title of the invention: ORDERED DELIVERY OF INTERCEPTED DATA  
Titre de l'invention:

Anmeldetag:  
Date of filing: 07 September 1999 (07.09.99)  
Date de dépôt:

In Anspruch genommene Priorität(en)  
Priority(ies) claimed  
Priorité(s) revendiquée(s)

Staat:	Tag:	Aktenzeichen:
State:	Date:	File no.
Pays:	Date:	Numéro de dépôt:

Benennung von Vertragsstaaten : Siehe Formblatt PCT/RO/101 (beigefügt)  
Designation of contracting states : See Form PCT/RO/101 (enclosed)  
Désignation d'états contractants : Voir Formulaire PCT/RO/101 (ci-joint)

Bemerkungen:  
Remarks:  
Remarques:

## PCT REQUEST

WO 25069

Original (for SUBMISSION) - printed on 07.09.1999 04:04:55 PM

IV-1	<b>Agent or common representative; or address for correspondence</b> The person identified below is hereby/has been appointed to act on behalf of the applicant(s) before the competent International Authorities as:	agent
IV-1-1	Name (LAST, First)	PELLMANN, Hans-Bernd
IV-1-2	Address:	Tiedtke-Bühling-Kinne Bavariaring 4 D-80336 Munich Germany
IV-1-3	Telephone No.	+89 54 46 90
IV-1-4	Facsimile No.	+89 53 26 11
IV-2	Additional agent(s)	additional agent(s) with same address as first named agent
IV-2-1	Name(s)	TIEDTKE, Harro; BÜHLING, Gerhard; KINNE, Reinhard; GRAMS, Klaus; LINK, Annette; VOLLNHALS, Aurel; LESON, Thomas, Johannes, Alois; TRÖSCH, Hans-Ludwig; CHIVAROV, Georgi; GRILL, Matthias; KÜHN, Alexander; OSER, Andreas; BÖCKELEN, Rainer
V	<b>Designation of States</b>	
V-1	<b>Regional Patent</b> (other kinds of protection or treatment, if any, are specified between parentheses after the designation(s) concerned)	AP: GH GM KE LS MW SD SZ UG ZW and any other State which is a Contracting State of the Harare Protocol and of the PCT EA: AM AZ BY KG KZ MD RU TJ TM and any other State which is a Contracting State of the Eurasian Patent Convention and of the PCT EP: AT BE CH&LI CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE and any other State which is a Contracting State of the European Patent Convention and of the PCT OA: BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG and any other State which is a member State of OAPI and a Contracting State of the PCT
V-2	<b>National Patent</b> (other kinds of protection or treatment, if any, are specified between parentheses after the designation(s) concerned)	AE AL AM AT AU AZ BA BB BG BR BY CA CH&LI CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZA ZW

ORDERED DELIVERY OF INTERCEPTED DATAField of the invention

- 5 The present invention relates to a method and a system  
for performing a lawful interception in a packet network.

BACKGROUND OF THE INVENTION

- 10 The provision of a lawful interception is a requirement  
of national law, which is usually mandatory. From time to  
time, a network operator and/or a service provider will  
be required, according to a lawful authorization, to make  
15 results of interception relating to specific identities  
available to a specific intercepting authority or Law  
Enforcement Agency (LEA).

- There are various aspects of interception. The respective  
20 national law describes under what conditions and with  
what restrictions interception is allowed. If an LEA  
wishes to use lawful interception as a tool, it will ask  
a prosecuting judge or other responsible body for a  
lawful authorization, such as a warrant. If the lawful  
25 authorization is granted, the LEA will present the lawful  
authorization to an access provider which provides access  
from a user's terminal to that network, to the network  
operator, or to the service provider via an  
administrative interface or procedure. When a lawful  
30 interception is authorized, an Intercept Related  
Information (IRI) and/or the content of the corresponding  
communication (CC) is delivered to the LEA.

- The lawful authorization may describe the IRI and the  
35 content of the communication that are allowed to be

delivered for this LEA., Typically, the interception period and interception target (e.g., a person's name or MSISDN number(s) related to SIM card(s) or IMEI code of a mobile terminal. For different LEAs and for different

5 investigations, different constraints can apply that further limit the general borders set by the law. The interception target may also be described in different ways in a lawful authorization, e.g. subscriber address, physical address, location, services etc.

10

Such a lawful interception functionality is also needed in the packet switched part of new mobile data networks such as the GPRS and the UMTS.

15 Lawful interception is based on an EU Council resolution, which concerns all telecommunications systems, not only mobile ones. The European Telecommunications Standards Institute (ETSI) has defined further technical requirements. These requirements define three interfaces:

20

X0\_1 (=HI1): administrative tasks (may be on paper or fax or online or otherwise)

X0\_2 (=HI2): network signaling (near real time)

X0\_3 (=HI3): intercepted user data (near real time)

25

The interface X0\_1 carries interception requests, authorization documents, encryption keys and the like.

The interface X0\_2 carries IRI (Interception Related Information) like phone numbers, service information,

30 time stamps etc. The interface X0\_3 carries the content of communication (CC), i.e., the intercepted packets containing data sent and/or received etc. The exact definitions of the three interfaces are left to local

legislation and authorities. The interfaces X0\_1 to X0\_3

35 are referred in the GSM 03.03 (where GPRS annex was

included June 1999). The three X0 interfaces are defined in ETSI ES 201 671 V1.1.1 as HI1/HI2/HI3 interfaces, wherein symbols X0\_1 to X0\_3 correspond to HI1 to HI3, respectively.

5

With respect to Fig. 1, the lawful interception is described in more detail. Fig. 1 shows a reference configuration for the lawful interception for GPRS (General Packet Radio Systems). Reference numeral 1  
10 denotes a Law Enforcement Agency (LEA) mentioned above. The symbols X0\_1, X0\_2 and X0\_3 denote the above mentioned interfaces between the LEA and respective network elements which are described in the following. Numeral 2\_1 denotes an Administrative Function for LI  
15 (Lawful Interception) in the network. Numeral 2\_2 indicates an IRI delivery function (also known as DF2P for packet data like GPRS), whereas numeral 2\_3 indicates a CC delivery function (also known as DF3P for packet data). The ADMF 2\_1, the IRI delivery function 2\_2 and  
20 the CC delivery function 2\_3 are connected to a GSN (GPRS Support Node) 3 via interfaces X1\_1p, X2p and X3p. In addition, the IRI and CC delivery functions are connected with the ADMF 2\_1 via interfaces X1\_2p and X1\_3p, respectively. The GSN 3 can be a SGSN or a GGSN or other  
25 node intercepting user activity or frames containing user level packet data.

In this manner, the ADMF 2\_1 is used together with the delivery functions to hide from the GSN that there might  
30 be multiple activations by different Law Enforcement Agencies (LEAs) on the same target. Additionally, the packet network complexity is hidden from the LEA(s).

The above described LI structure works satisfactorily in  
35 case of circuit switched services like GSM. However, the

situation is different for packet switched services like GPRS.

That is, in case of a packet switched services, the IRI  
5 and CC data are transmitted in packets to the LEA 1. The  
packet flow starts from the packet intercepting node  
(i.e. , GSN 3 in Fig. 1) to the delivery function nodes  
(i.e., IRI and CC delivery functions 2\_2 and 2\_3 in Fig.  
1) to the LEA 1. The LEA system has a mass memory for  
10 packets, but it may also monitor packets as near real  
time streams. In GPRS, for example, the IRI data is  
defined to have some network attachment and/or PDP  
(Packet Data Protocol) context related data incorporated  
that relates the IRI to certain subscriber activity. The  
15 packets relate to a certain PDP context.

In the packet switched networks as described above, there  
is a possibility that due to delay changes in the  
networks, e.g., because of handovers, packets are  
20 received in a different order than they were sent. In  
other words, user data (CC) relating to a single  
communication session (PDP context in GPRS networks) may  
be routed via different nodes towards a delivery function  
and finally to the LEA due to handovers (like SGSN  
25 handovers in GPRS networks) or Network Element (NE)  
redundancy cases where NE2 takes over the responsibility  
of another NE1 of similar kind, due to capacity or NE  
failure reasons. Hence, it is possible that the packets  
(either IRI or CC) sent from the SGN 3 to the LEA will  
30 arrive in a different order than that in which they were  
actually sent.

It is known that packets can be numbered to allow the  
reconstruction of the actual packet order. However, in  
35 Lawful Interception (LI) it may not be enough to only



reconstruct the actual order of packets itself. By contrast, it is also important to know which IRI packets relates to which CC packet. Since IRI packets and CC packets are transmitted via logically separate  
5 connections to the LEA and the number of CC and IRI packets are typically not 1:1, it is difficult to relate the two kind of packets to each other in an efficient way. Hence, if in LI such delays and misorders of IRI and/or CC packets occur, this will cause serious problems  
10 since organizing the packets afterwards into a correct order is a more complicated task than getting them in an easily identifiable order from the first possible point.

#### SUMMARY OF THE INVENTION

15

Therefore, the object underlying the invention resides in providing a method and a system by which missequenced information packets can be avoided.

20

According to the invention, this object is solved by a method according to claim 1. In particular, according to the invention a method for performing a lawful interception in a packet network is provided, which comprises the steps of:

25

generating interception related information packets from a communication to be intercepted;

generating communication content packets from a communication or network activity to be intercepted;

30

providing identification data for the interception related information packets and for the communication content packets of one group of communication packets;

providing ordering data for each of the interception related information data packets and for each of the communication content packets; and

transmitting the interception related information packets, the communication packets, the identification data and the ordering data to an interception authority device .

5

Alternatively, the above object is solved by an interception system for packet networks according to claim 10. The interception system comprises

at least one first network element for intercepting  
10 a communication; and

at least one interception authority device; wherein the first network element comprises

a first packet generating means for generating interception related information packets from a  
15 communication to be intercepted;

a second packet generating means for generating communication content packets from the communication to be intercepted;

an identification data generating means for  
20 generating an identification data for the interception related information packets and the communication content packets associated to the communication or network activity;

a first ordering data generating means for  
25 providing ordering data for each of the interception related information data packets;

a second ordering data generating means for providing ordering data for each of the communication content packets; and

30 a transmitting means for transmitting the interception related information packets and the communication content packets including the correlation data to the interception authority device.

Thus, by the method and the system according to the invention, the received IRI and CC packets can easily be put in the correct time order.

5 Therefore, performance increases in the receiving end system, i.e., the Lawful Enforcement Monitoring Facility (LEMF) of the LEA, as less operation load is necessary for determining the correct order of the packets received.

10

Furthermore, the reliability of the detected communication content (CC) increases, since the order of the CC packets is correct.

15 Moreover, also missing or duplicated IRI and CC packets can be noticed. Time stamps would not alone show LEA if some packets were lost. Additionally, time stamp decoding consumes more processing power than sequence number checking.

20

In addition, the assembly of IRI packets between corresponding CC packets is possible by LEMF. That is, although IRI and CC packets are transmitted via logical separate channels, the LEMF can recognise the exact order

25 and correlation of IRI and CC packets to each other.

Now e.g. the problems relating to handovers of intercepting nodes (such as SGSNs in GPRS) and the asynchronous transmission of those packets through the network between the intercepting nodes and the DF/LEA system(s), and the possible unpredictable time order of e.g. the packets sent near a intercepting node handover could be avoided without much extra processor work.

30 Furthermore, the LEMF can this way detect lost or duplicated IRI/CC packets (Such kind of situations could

35

arise in redundancy cases when a NE2 (second network element) takes over the tasks of a NE1 (first network element) due to a NE1 failure or due to capacity or other reasons. Also, the relation of IRI packets and the  
5 corresponding CC packets could be based on this same numbering, resulting in better processor efficiency than e.g. inspecting the higher layer protocol packet numberings which could even vary and be in future something else than was in use in that time the current  
10 design of the LI system was done.

In most time measurement cases in telecommunication, the precision is limited, e.g., to 1 second. Then it could occur that two or more packets get the same time stamp  
15 (or a very, very precise but also very processor inefficient time keeping system would be needed. Sequence numbers offer also in this respect a better way for providing packets.

20 Further advantageous developments are set out in the dependent claims.

In particular, the identification data can be used for identifying interception related information (IRI)  
25 packets and for identifying the communication content (CC) packets of the communication, and the ordering (sequence number) data can be used for ordering the IRI packets and the CC packets. As mentioned above, the process for putting the packets in the correct time order  
30 can be simply performed by rearranging the received packets in a suitable memory.

The identification data can be a session identification data. Specifically, in case the network is a GPRS packet  
35 network, the CC session identification data can be

obtained from the PDP context table of the serving GSN and the IRI identification data for a user can be retrieved from the GPRS attached mobiles of the serving SGSN and/or PDP context data of a serving GSN.

5

The ordering data can be integer numbers which are incremented for each sequential packet. Hence, a sequential order can easily be provided. The sequential number should have an enough large maximum value, e.g.  
10  $2^{64}$ . The maximum sequence number would be reached only after an extremely long time period, and then it could be allowed to start from 0 again, as the LEA would not any more have the older packets as uninspected. (Those packets would have been deleted using, e.g., an automatic  
15 timeout or deletion policy (by LEMF) for very old sequence numbers. For completeness, the newest packets overlapping the maximum sequence number could have a flag to indicate (in record sequence number order comparison situations) that they are newer (greater) than the old  
20 tail of sequence numbers that is after a sequence number range overflow only approaching the overflow situation.

Furthermore, a time stamp could even be provided to each IRI packet and/or to each CC packet. The time stamp can  
25 have a precision of one second, for example, or any other suitable value. By this measure, only a limited number of ordering data is necessary. In particular, by using this time stamp also the flag mentioned above could be omitted.

30

Moreover, for each IRI packet and each CC packet, a frame can be provided in which the identification data and the ordering data can be included. In addition, if a time stamp is provided, also the time stamp can be included in  
35 the frame. By this measure, the packets are provided with

a unique format in which all necessary values and identifiers can easily be read at the packet receiving side.

5

#### BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be more readily understood with reference to the accompanying drawings in which:

10

Fig. 1 shows schematically a network system comprising a LEA and an interception node of a network, to which the invention can be applied,

15 Fig. 2 shows schematically the structure of an IRI or CC packet according to an embodiment,

Fig. 3 shows parts of the interception node according to the embodiment,

20

Fig. 4 shows parts of the LEA according to the embodiment,

Fig. 5 shows a flowchart of a process for synchronising  
25 IRI packets and CC packets according to the embodiment,

Fig. 6 shows a flowchart of a routine performed in step S6 of Fig. 5, and

30 Fig. 7 shows a flowchart of a process for receiving the IRI and CC packets according to the embodiment.

#### DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

35

In the following, a preferred embodiment of the invention is described in more detail with reference to the accompanying drawings.

5 Fig. 1 shows a network system to which the embodiment is applicable. Since Fig. 1 has already been described in the introductory part, an unnecessary repetition is omitted here. However, it is noted that the interception node, i.e., the GSN 3, and the LEA 1 are modified  
10 according to the embodiment, as will be described later.

According to the invention, the IRI packets (relating to intercepted packet switched communication content or circuit switched communication content) are sequence  
15 numbered, e.g. by starting from 0 and incrementing packet by packet. Similarly, the CC packets related to a certain communication session (e.g. PDP context in GPRS), are sequence numbered. Thus the IRI packets IRI0, IRI1, IRI2, ... IRI<sub>n</sub> received by the IRI and CC delivery functions  
20 2\_2 and 2\_3 and/or LEA 1 (relating to a certain communication session) appear in an order, from which the actual communication content (CC) data can be taken by the LEA 1 in the correct order. The same applies to the CC packets CC0, CC1, CC2, ... CC<sub>m</sub> that relate to a  
25 certain communication session.

That is, according to the embodiment of the invention, the IRI and CC packets are provided with a session identifier for identifying the communication session to  
30 be intercepted (between, eg., one of the communication processes of an end terminal (e.g., Mobile Station, MS) and a network Access Point, AP) and packet order numbers for ordering the packets in the correct time order. Fig. 2 shows schematically an example for an IRI or CC packet.  
35 Here, a frame has been generated and the session

identifier and the packet order number has been inserted in the header of the frame, besides further control data like the address etc. Optionally, also a time stamp can be provided in the header of the packets. The packet body  
5 comprises the actual intercepted data.

Fig. 3 shows the interception node (GSN, i.e., GPRS Support Node) 3 in more detail. It is noted that this can be a SGSN (Serving GPRS Support Node), a GGSN (Gateway  
10 GPRS Support Node) or any other suitable node which can be used for incorporating an interception function therein. Reference numerals 31 denotes the GSN node itself, which is adapted to intercept a communication performed via the corresponding GPRS (packet switched)  
15 network. Reference numerals 32 and 33 denote an IRI detector and a CC detector, respectively.

The IRI detector 32 is adapted to detect the necessary interception related information associated to the  
20 communication to be intercepted and creates data packets (as shown in Fig. 2) in which the interception related information (IRI) is included in the user data and in which the header provides room for the session identifier and the order number.

25 Likewise, the CC detector 33 is adapted to detect the communication contents of the communication to be intercepted and creates data packets (as shown in Fig. 2) in which the communication data is included in the user  
30 data (e.g. intercepted IP packet header and payload contents) and in which the header provides room for the session identifier and the order number.

An identifier generator 34 is provided to set an session  
35 identifier (identification number) in the corresponding



header field of the CC and IRI packets. In ETSI ES 201  
671 v1.1.1 a similar parameter is the Call Identifier  
(CID), consisting of the Network Identifier (NID) and the  
Call Identity Number (CIN). The CIN identifies uniquely  
5 one logical network communication link between an user  
terminal and an other communication party behind or in a  
network. Thus, this identifier according to the PDP  
context can be used for the session identifier. However,  
also other identifier are possible, for example, an  
10 arbitrary number could be used.

Reference numerals 35 and 36 denote IRI and CC ordering  
means. These ordering means generate ordering numbers for  
the IRI and CC packets. In particular, when a new session  
15 to be intercepted starts, the order number for both  
packets is reset to 0. Then, for each new packet of both  
kinds, this order number is incremented, such that a row  
of IRI packets IRI0, IRI1, . . . ., IRI<sub>n</sub> and a row of CC  
packets CC0, CC1, . . . , CC<sub>m</sub> are created. It should be  
20 noted that the order numbers for both kinds of packets  
are independent. That is, there is an IRI order number  
and a CC order number. There can be more CC packets than  
IRI packets, that is,  $n < m$ , or vice versa.

25 Reference numeral 37 denotes a transmitter which  
transmits the CC packets and the IRI packets via the  
network to the LEA 1.

According to this embodiment, also a time stamp means 38  
30 is provided. This time stamp means 38 provides a time  
stamp having, e.g., the precision of a second into the  
header of the frame of the CC and IRI packets. In  
principle, the time stamp means 38 can be connected to  
every part of the interception node 3, as long as the  
35 time stamp can be provided before transmitting the IRI

and CC packets. However, preferably the time stamp means 38 is provided between the identifier generator 34 and the IRI and CC ordering means 35 and 36.

5 The IRI and CC packets are transmitted, via the packet switched network, to the Law Enforcement Agency (LEA) device 1. The parts of the LEA 1 relating to the preferred embodiment of the invention are shown in Fig. 4. The IRI packets and the CC packets are received via  
10 the interfaces X0\_2 and X0\_3, respectively, by a receiver 11. Due to the further control data (i.e., address data) the receiver 11 is able to distinguish between the IRI and CC packets. An identifier detector 12 is adapted to detect the session identifier according to the  
15 communication to be intercepted, such that all packets related to one communication session can be arranged together. The ordering of the IRI packets and CC packets in the correct time order is performed by the IRI and CC packets 13 and 14, optionally by taking into account the  
20 time stamp.

For rearranging the received packets, the ordering means 13 and 14 should have a suitable memory, i.e., a RAM with a large capacity. If there will be likely less IRI  
25 packets than CC packets, the RAM need for the IRI ordering means 13 can be smaller than that of the CC ordering means 14.

Thus, the IRI packets and the CC packets can be output in  
30 the correct time order and in correct correlation to each other. That is, for each communication session, CC packets and IRI packets can be investigated in the correct order.

The method according to the invention is described in the following with respect to the flowcharts shown in Figs. 5 to 7.

5 Fig. 5 shows a process for synchronising IRI and CC packets according to the invention. In step S1, an LI (Lawful Interception) request is issued by the LEA 1. This request is transmitted via the interface X0\_1, the ADMF 2\_1 and the interface X1\_1p shown in Fig. 1 to the  
10 interception node (GSN) 3. In step S1, the process is started and initialised. In particular, ordering numbers used for IRI and CC packets are reset, that is, the IRI order number is reset to 0 and the CC order number is reset to 0.

15

The following steps S2 to S7 are repeated for every packet which is generated during the interception.

In step S2, a packet is generated, which can either be an  
20 IRI packet or a CC packet. As mentioned above, the IRI packet contains information related to the interception, which could be e.g., telephone number, Lawful Interception Identifier (LIID), which is agreed between LEA and the NMO/AP/SvP (see e.g. ES 201 671 v1.1.1) etc.,  
25 whereas the CC packet contains at least the content of the actual communication which is intercepted. In steps S2, also the data frame as shown in Fig. 2 is generated.

In step S3, a session identifier is provided. According  
30 to this embodiment, the PDP context in GPRS is used for determining the session identifier, as described above.

In step S4, a time stamp is provided. As described above, this step is optional and can be left out, if not  
35 necessary. If used, the time stamp is provided in the

corresponding field of the header of the CC or IRI packet as shown in Fig. 2.

In step S5, the packet order number is generated. In  
5 principle, this is performed by incrementing a general order number during each loop and taking the current value of this order number as the packet order number. It is noted that there have to be two independent order numbers, one for IRI packets and one for CC packets. The  
10 process carried out in this step is later on described in more detail with respect to Fig. 6.

In step S6, the packet is transmitted to the LEA via the network by using the interfaces as shown in Fig. 1.  
15

In step S7 it is investigated whether the current Lawful Interception (LI) is completed or whether it has to be continued. If the interception is to be continued, the process returns to step S2. If the current LI is to be  
20 completed (i.e., a request for ending the current LI has been received), the process is ended.

Next, a routine to generate the packet order number carried out in step S5 is described in more detail.  
25 First, in step S51, it is distinguished whether the packet in question is an IRI packet or a CC packet. Since the following operations for the IRI packets and the CC packets basically correspond to each other, only steps S52 to S55 with respect to IRI packets are describe in  
30 order to simplify the description.

In step S52 it is determined whether the first IRI event (see GSM 03.03. for GPRS) for a session has been generated by the intercepting node. If so, the routine  
35 advances to step S53 in which the IRI number is reset to

0. If the time stamp is unchanged, the IRI order number is incremented in step S54. In step S55, the IRI order number is taken as the packet order number and set in the header of the IRI packet (cf. Fig. 2). After that, the  
5 routine returns to the process shown in Fig. 5.

In case the actual packet is a CC packet, steps S56 to S59 are carried out in a similar manner as that according to steps S52 to S55. Hence, a further description thereof  
10 is omitted.

Next, the process carried out by receiving the CC packets and the IRI packets by the LEA 1 is described with respect to Fig. 7.

15

In step S10, the IRI and CC packets from the GSN 3 (i.e., the interception node) are received via the interface X0\_2 and X0\_3, respectively. In step S11, the session identifier which indicates the communication session  
20 intercepted is detected. This is performed by reading the corresponding value from the header of the packet, as shown in Fig. 2. Then, the IRI packets and the CC packets associated to the session identified by the session identifier are distinguished in step S12.

25

Then, in step S13 the packets associated to this session are arranged in the correct time order. This is effected by detecting the corresponding IRI or CC order number in the header of the packet and by arranging the packets  
30 according to the order numbers.

Finally, the communication session intercepted which is represented by the sequence of CC packets can be investigated in step S14. That is, a recording of this

communication, a search for key words or the like, etc.  
may be performed.

As an alternative to the above-described embodiment, the  
5 providing of the session identifier could be modified.  
Often it could be that there are much more CC packets  
than IRI packets. Hence, according to this modification,  
the IRI packets could be provided with a reference number  
to the previous CC packet generated before the IRI  
10 packet. (other alternative is that the CC packets would  
have reference number to the last IRI packet generated by  
this node for this session.) In this case, the time stamp  
might be even omitted. Nevertheless, both CC and IRI  
packets could be provided with the session identifier,  
15 which could be derived from, e.g., the PDP context, and  
Node ID in GPRS.

As a further alternative of the above-described preferred  
embodiment, the elements shown in Fig. 4 could also be  
20 incorporated in the ADMF 2\_1, the IRI delivery function  
means 2\_2 and the CC delivery function means 2\_3 such  
that arranging of the CC and IRI packets in the correct  
order is already performed in the DF (delivery function)  
which is provided by the means 2\_1 to 2\_3. This reduces  
25 the load for the LEA. Furthermore, an LEA not having the  
means shown in Fig. 4 can easily be supplied with ordered  
data.

It is noted that the term communication session do not  
30 only refer to an active communication, but also to a case  
where a mobile station is passive, i.e., in which the  
mobile station only waits for an answer but is connected  
to the network.

35 In the following, a second embodiment is described.

As mentioned above, the IRI packets and/or the CC packets are provided with sequence numbers. The maximum sequence number is preferably chosen so high that normal

5 communication can be intercepted without an overflow of the sequence numbers.

However, they might occur situations in which the numbers are getting so high that an overflow takes place. For  
10 example, this can happen in case a mobile station is permanently online. For example, a bottle vending machine could have a permanent connection to a central point. In this case, it should be possible to distinguish between packets having sequence numbers before the overflow and  
15 packets having sequence numbers after the overflow. In the first embodiment, this situation is handled by the flag.

However, according to the second embodiment, the flag is  
20 replaced by an other indication. For example, the indication could be a colour. That is, a first row of packets can be assigned the colour "green". Then, in case an overflow takes place, the packets with the new numbers can be assigned the colour "blue". Thus, the packets of  
25 the row before the overflow can easily be distinguished from packets having numbers after the overflow, although the new sequence numbers are smaller than the old sequence numbers. That is, the "green" packets can easily be recognised as old packets (generated before the  
30 overflow), whereas the "blue" packets can easily be recognised as new packets (generated after the overflow).

As an alternative, the old packets could also be assigned with a different colour, e.g., "red". By this measure, it

is clear that an overflow has taken place and that these packets are old packets.

If then another overflow takes place, the situation is reversed, such that now the old packets are "green" and the new packets are "blue". In this way, the provision of the packets can be continued endlessly.

It is to be understood that the indication by colours is only an example for the overflow indication. There are also other forms of indications possible, for example predetermined integer values, characters or the like. It is also possible to provide a flag for distinguishing between old and new packets, and to provide an extra flag in case an overflow has taken place. This extra flag could be reset in case no more old packets are present.

The above described embodiment can be preferably used in the structure and method according to the first embodiment and modifications thereof. However, the second embodiment is not limited thereto. In particular, it is not limited to the above structure of two different data packets (i.e., IRI and CC packets) according to the first embodiment. The measure according to the second embodiment can also be applied to a data packets of a single kind which have to be put in an order.

The above description and accompanying drawings only illustrate the present invention by way of example. Thus, the embodiments of the invention and the modifications thereof may vary within the scope of the attached claims. For example, the embodiments and the modifications thereof can be combined.



### Claims

1. A method for performing a lawful interception in a  
5 packet network, comprising the steps of:  
generating (S2) interception related information  
packets from a communication or network activity to be  
intercepted;  
generating (S2) communication content packets from  
10 said communication or network activity to be intercepted;  
providing (S3) identification data for said  
interception related information packets and for said  
communication content packets of one group of  
communication packets;  
15 providing (S5) ordering data for each of said  
interception related information data packets and/or for  
each of said communication content packets; and  
transmitting (S6) said interception related  
information packets, said communication packets, said  
20 identification data and said ordering data to an  
interception authority device (1).
2. The method according to claim 1, further comprising  
the steps of  
25 using (S11, S12) said identification data for  
identifying interception related information packets and  
for said communication content packets of said one group  
of communication packets; and  
using (S13) said ordering data for ordering said  
30 interception related information packets and said  
communication content packets.
3. The method according to claim 1, wherein said  
identification data is a session identification data.

4. The method according to claim 3, wherein said packet network is a GPRS network and said session identification is data is obtained from a PDP context in GPRS.
- 5 5. The method according to claim 1, wherein said ordering data are integer numbers which are incremented for each sequential packet.
6. The method according to claim 1, further comprising  
10 the step of providing (S4) a time stamp to each interception related information packet and/or to each communication content packet.
7. The method according to claim 1, further comprising  
15 the step of  
providing (S2) a frame for each interception related information packet and each communication content packet, in which said identification data and said ordering data is included.
- 20 8. The method according to claim 7, further comprising the steps of  
providing a time stamp (S7) to each interception related information packet and/or to each communication  
25 content packet; and  
arranging said time stamp in said frame.
9. The method according to claim 1, wherein said ordering data are such that an overflow thereof is  
30 possible, and  
said method further comprises the step of  
providing a packet group indication to each interception related information packet and/or to each communication content packet for distinguishing between

the group of packets before said overflow and the group of packets after said overflow.

10. An interception system for packet networks,  
5 comprising

at least one first network element (3) for intercepting a communication; and

at least one interception authority device (1);  
wherein said first network element (3) comprises

10 a first packet generating means (32) for generating interception related information packets from a communication or network activity to be intercepted;

a second packet generating means (33) for generating communication content packets from said  
15 communication or network activity to be intercepted;

an identification data generating means (34) for generating an identification data for said interception related information packets and said communication content packets associated to said  
20 communication;

a ordering data generating means (35, 36) for providing ordering data for each of said interception related information data packets and/or each of said communication content packets; and

25 a transmitting means (37) for transmitting said interception related information packets and said communication content packets, said identification data and said ordering data to said interception authority device (1).

30

11. The system according to claim 10, wherein said interception authority device (1) comprises

a receiving means (11) for receiving said interception related information packets and said

communication content packets including said identification and said ordering data;

a identification means (12) for identifying interception related information packets and

5 communication content packets associated to said one communication; and

a packet ordering means (13, 14) for ordering said interception related information packets and/or said communication content packets according to said ordering  
10 data.

12. The system according to claim 10, wherein said identification data is a session identification data.

15 13. The system according to claim 12, wherein said network is a GPRS network and said identification data generating means (34) of said first network element (3) further comprises a session identification data detection means for detecting said session identification data from  
20 a PDP context.

14. The system according to claim 10, wherein said ordering data are integer order numbers and said ordering data generating means (35, 36) are adapted to increment  
25 the order number for each sequential packet.

15. The system according to claim 10, wherein said first network element further comprises

a time stamp generating means (38) for providing a  
30 time stamp to each interception related information packet and/or to each communication content packet.

16. The system according to claim 10, wherein said first network element comprises

a first frame generating means (32, 34) for providing a frame for each interception related information packet and for including said identification data in each frame, and

- 5 a second frame generating means (33, 34) for providing a frame for each communication content packet and for including said ordering data in each frame.

17. The system according to claim 16, wherein said first  
10 network element further comprises

a time stamp generating means (38) for providing a time stamp to each interception related information packet and/or to each communication content packet, wherein

- 15 said time stamp generating means (38) is adapted to include said time stamp into each of said frames.

18. The system according to claim 10, further comprising an interception related information packets  
20 delivering device (2\_2) for delivering said interception related information packets from said first network element (3) to said interception authority device (1);

a communication content packets delivering device (2\_3) for delivering said communication content packets  
25 from said first network element (3) to said interception authority device (1); and

a packet delivering control device (2\_1);

wherein said packet delivering control device (2\_1) is adapted to identify said interception related  
30 information packets and said communication content packets associated to said one group of communication packets on the basis of said identification data; and  
to order said interception related information packets and said communication content packets on the  
35 basis of said ordering data.

19. The system according to claim 10, wherein said ordering data are such that an overflow thereof is possible, and

5        said system further comprises a packet group distinguishing means for providing a packet group indication to each interception related information packet and/or to each communication content packet for distinguishing between the group of packets before said  
10 overflow and the group of packets after said overflow.

## Abstract

The invention discloses a method for performing a lawful interception in a packet network. The method comprises the steps of generating (S2) interception related information packets from a communication to be intercepted; generating (S2) communication content packets from a communication to be intercepted; providing (S3) identification data for the interception related information packets and for the communication content packets of one group of communication packets; providing (S5) ordering data for each of the interception related information data packets and for each of the communication content packets; and transmitting (S6) the interception related information packets, the communication packets, the identification data and the ordering data to an interception authority device. By this measure, a missequenced reception of interception related information (IRI) packets and communication content (CC) packets can be avoided. Also, the assembly of IRI packets between corresponding CC packets is possible by a corresponding LEMF of the interception authority.

(Fig. 5)

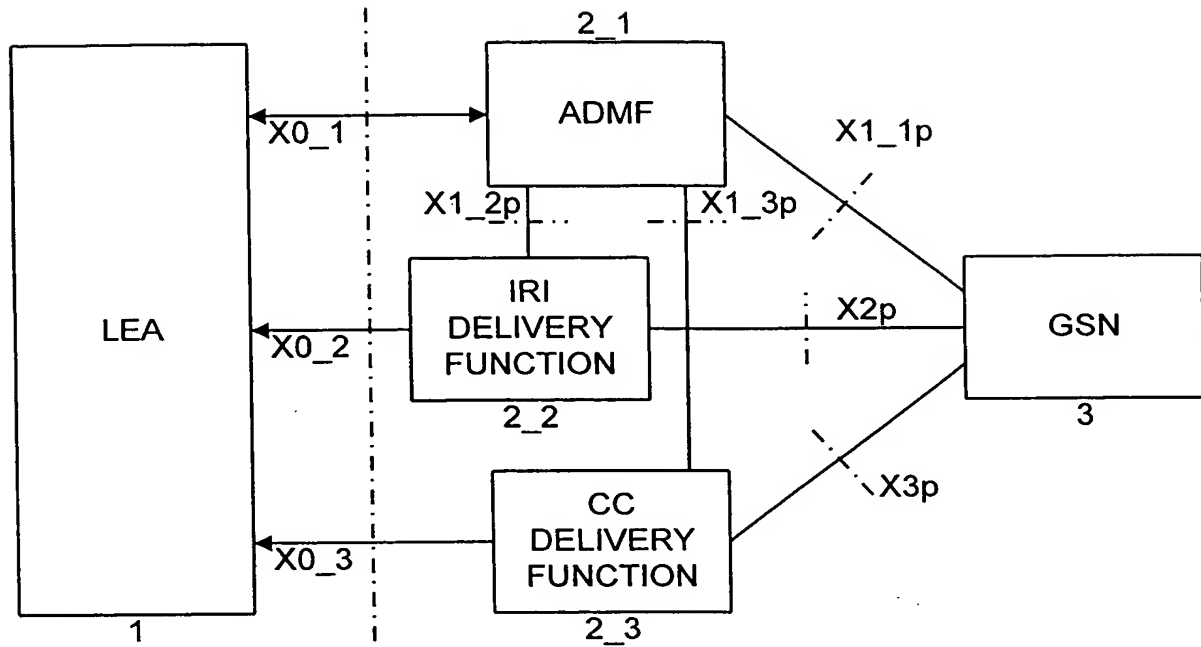


FIG. 1

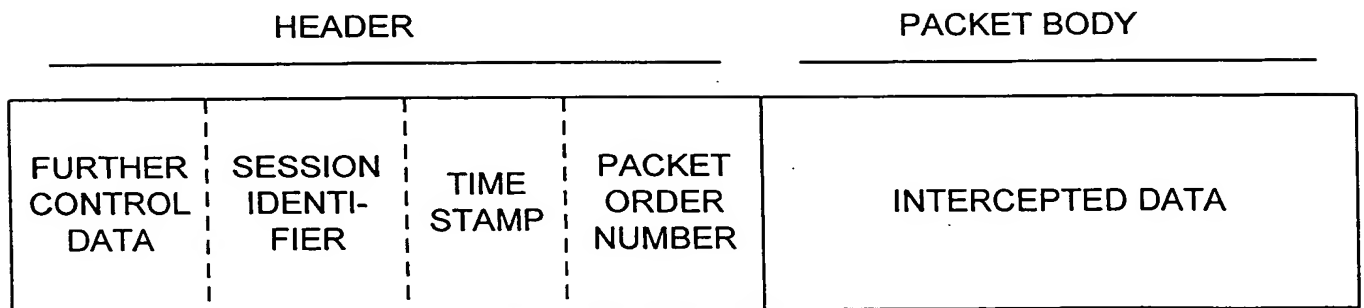
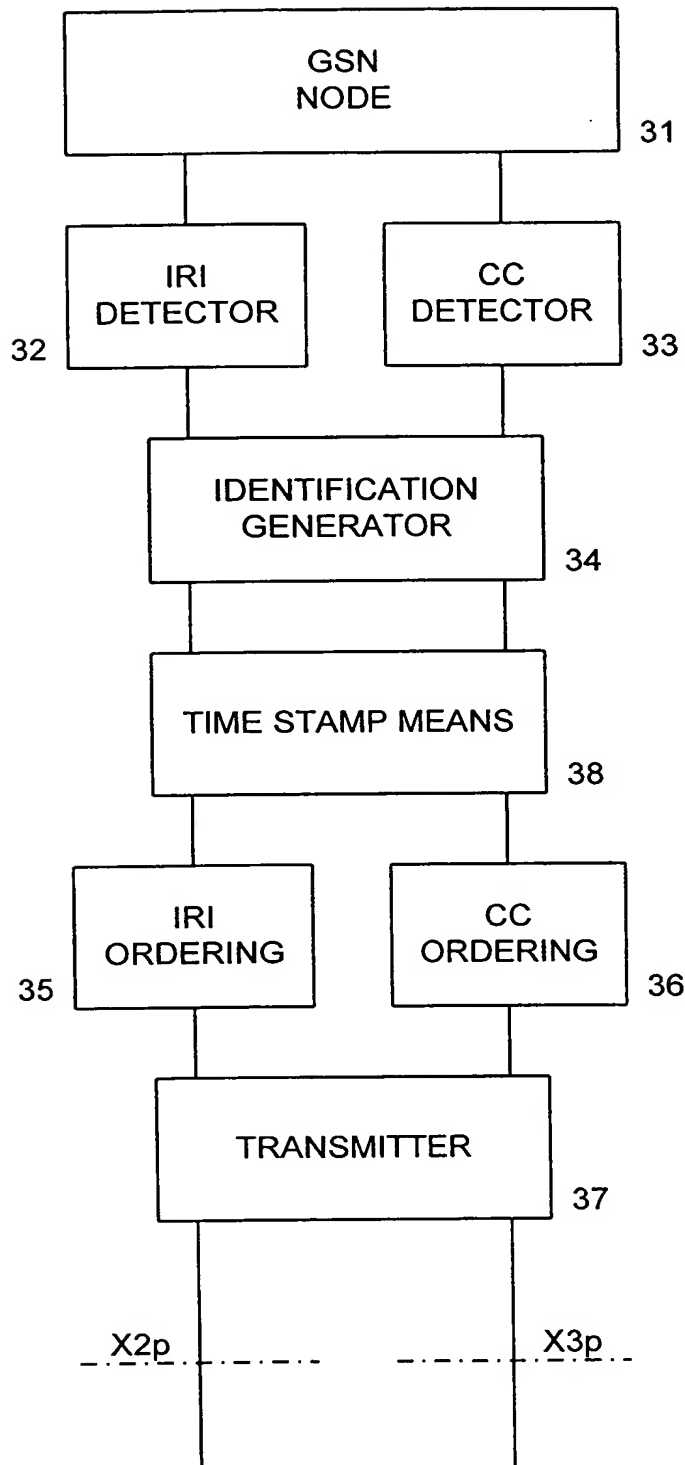
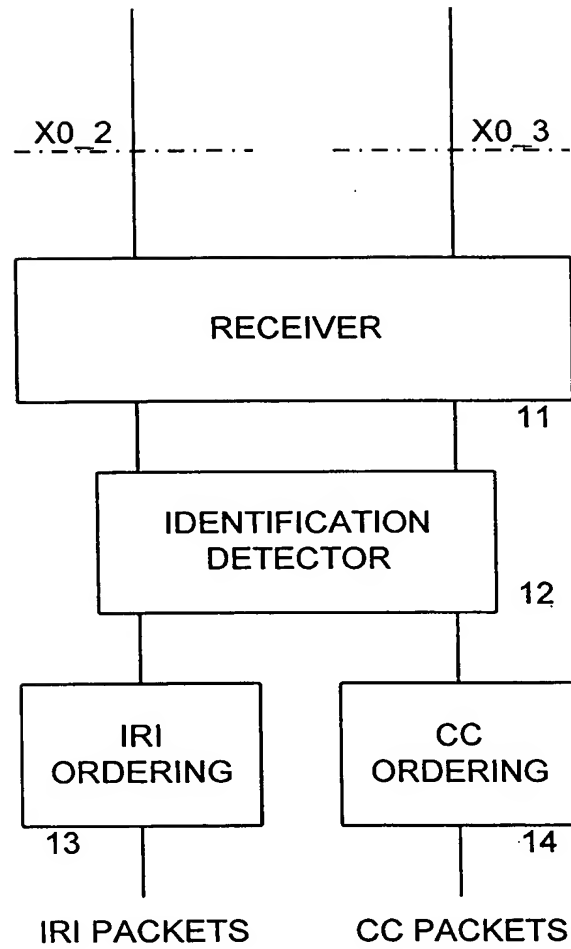


FIG. 2



**FIG. 3**

**FIG. 4**

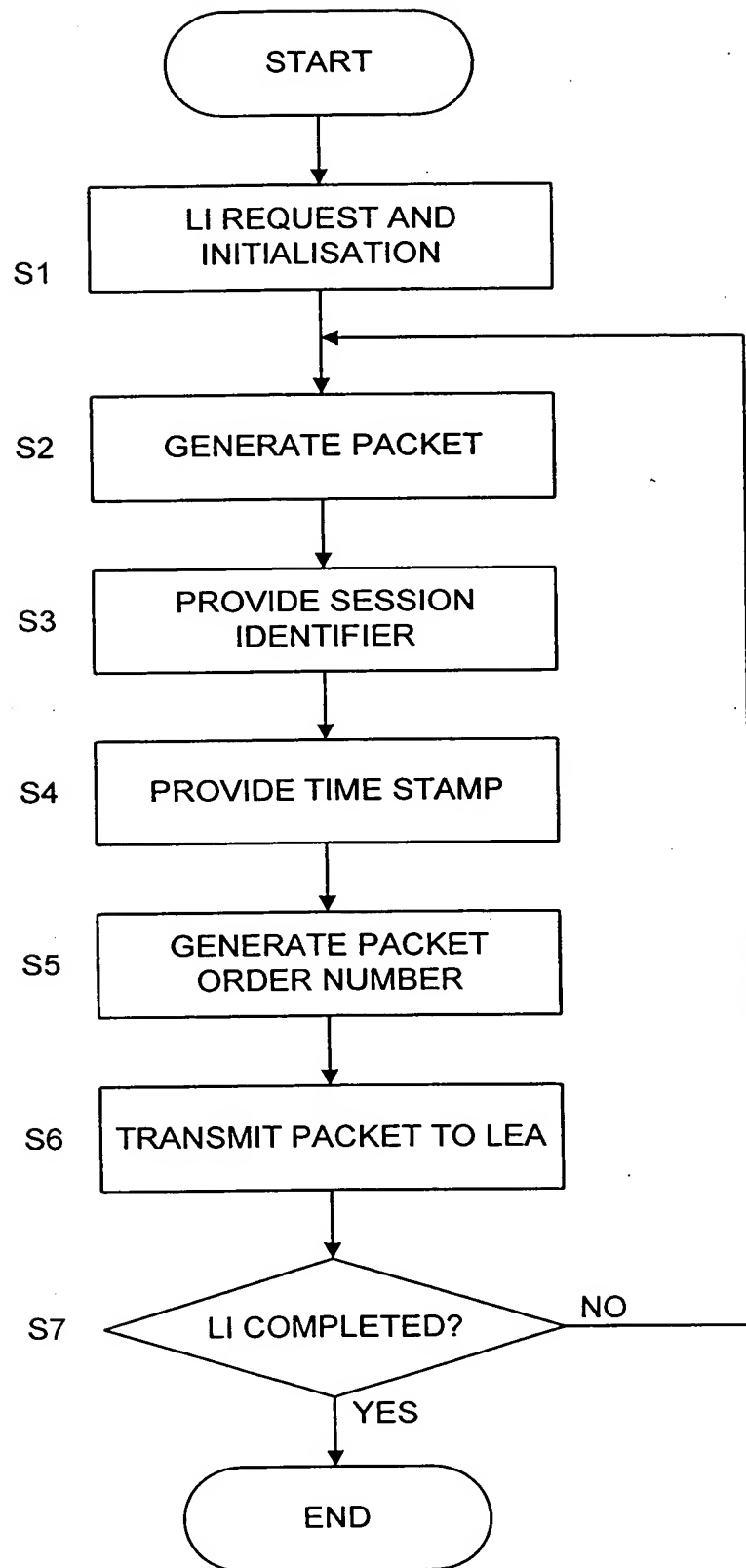


FIG. 5

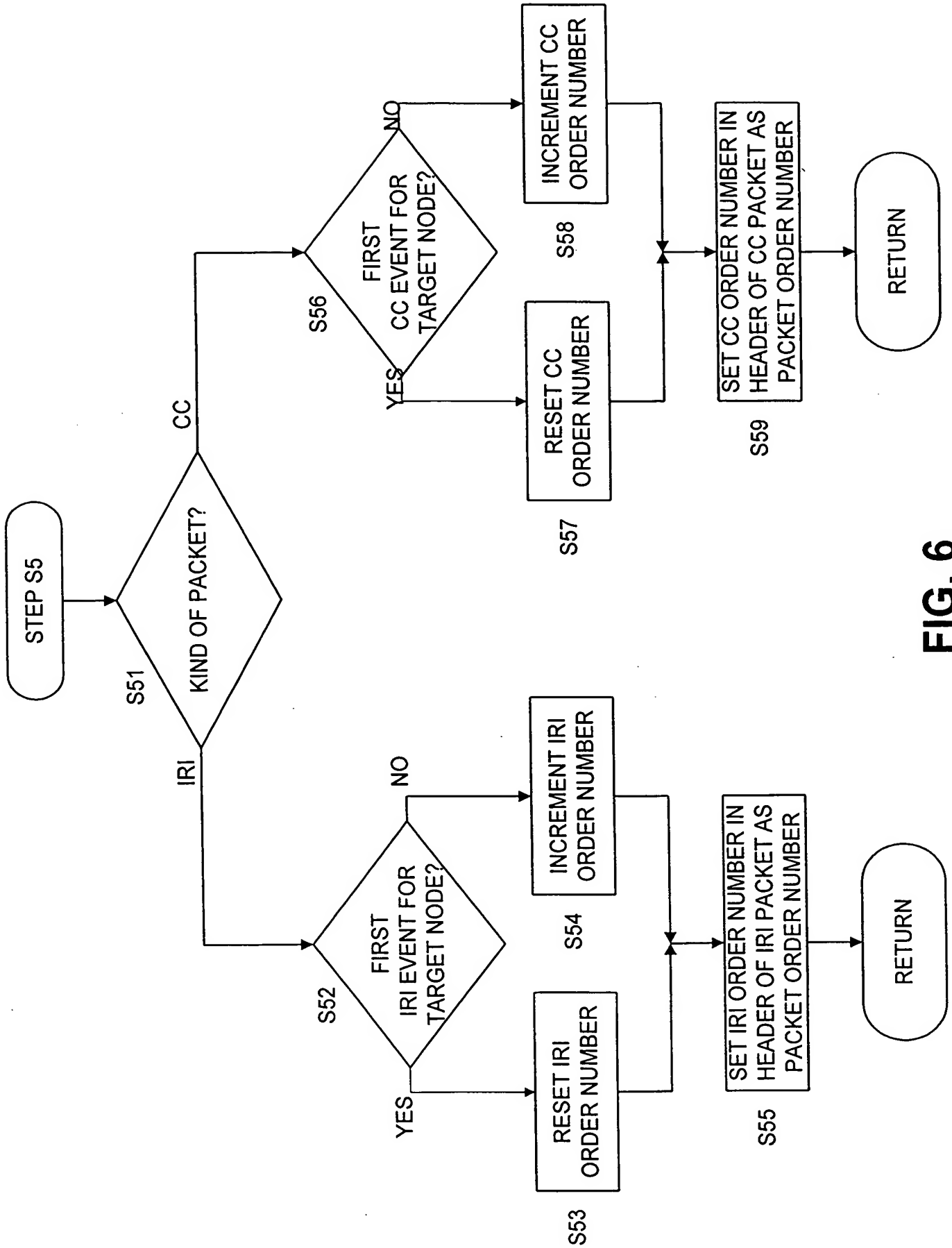
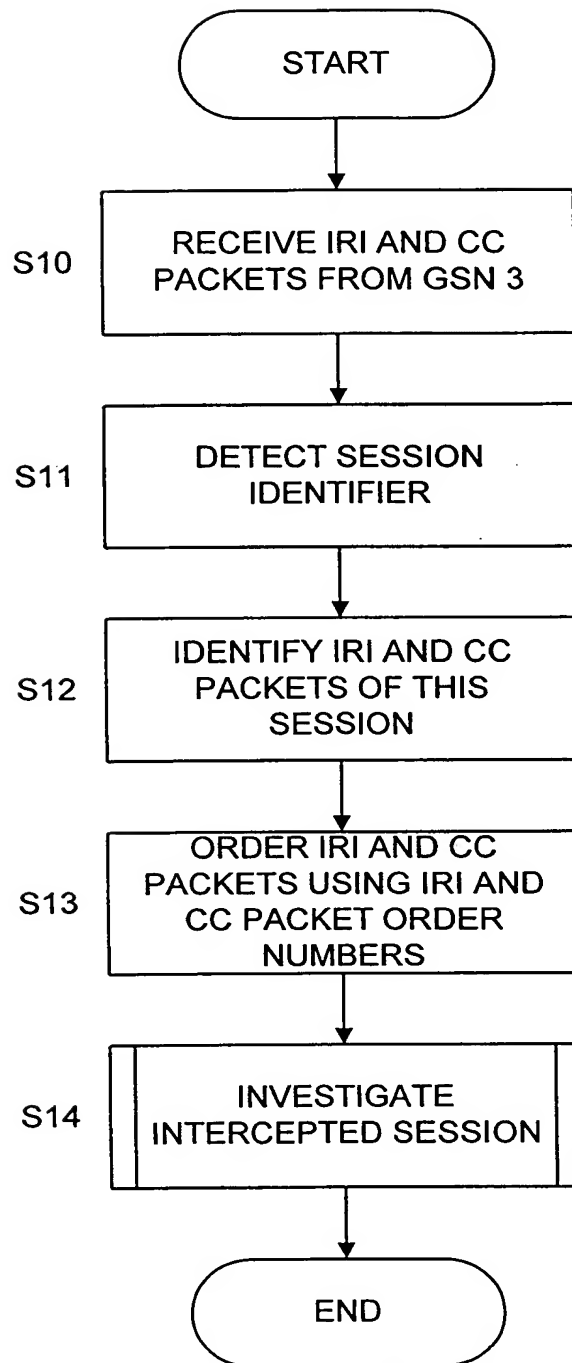


FIG. 6

**FIG. 7**